

REMARKS

Applicants acknowledge with thanks the Examiner's continued indication that claims 6-9, 13-15, 17 and 27 would be allowable.

The Examiner maintained the rejection of claims 2-3, 24-26 and 32-40 as being unpatentable over "RFC 2977 -- Mobile IP Authentication, Authorization and Accounting Requirements" (RFC 2977) in view of U.S. Patent Application Publication No. 2002/0065785 to Tsuda and further in view of U.S. Patent No. 6,751,459 to Lee *et al.*

In accordance with the Examiner's suggestion that "a more favorable outcome may occur if the applicant amends with the novel material as pointed out by the examiner" (see, for example, July 27, 2009, Advisory Action), Applicants amended independent claim 2 to include a feature based on the features recited in allowable claims 6 and/or 27, namely, the feature of transmitting to the subscriber's user equipment at least part of information required to obtain a certificate from the certificate provisioning gateway having the address of the certificate provisioning gateway. Applicants similarly amended independent claims 3, 24-26 and 32-35. Applicants also amended independent claims 2, 25 and 33 to remove some of the recited features that Applicants do not believe affect the patentability of the claims. Additionally, Applicants amended claims 6, 14 and 27 to make the language recited therein consistent with the amended language of independent claims 24, 26 and 25 from which claims 6, 14 and 27 respectively depend.

Applicants independent claim 2 recites "receiving, by a receiver, a message from subscriber's user equipment, said message indicating that an address of a certificate provisioning gateway for certificate issuance and delivery procedure in a visited network is requested by the subscriber's user equipment, the certificate provisioning gateway serving at least one certificate authority, ... determining, by the processor, on the basis of the subscriber's location information, an address of the certificate provisioning gateway; ... transmitting to the subscriber's user equipment at least part of information required to obtain a certificate from the certificate provisioning gateway having the address of the certificate provisioning gateway." Thus, the address of the certificate provisioning gateway that controls the issuance of certificates in the

visited network a subscriber's user equipment is located is determined, and at least part of the information required to obtain a certificate from the certificate authority in the visited network (via the certificate provisioning gateway) is transmitted to the subscriber's user equipment. For example, as described in the published application:

[0017] The new logical network node, authenticator AU, is a certificate provisioning gateway for the UE 4. The AU is a network node for the certificate issuing and delivery procedure. The AU may locate in a new physical node comprising only the AU or it may locate in a physical node comprising also another (other) logical network node(s). Typically each AU serves one CA. However, it is also possible that two or more CAs share one AU. The features of the AU-H 32 and/or the AU-V 22 in different embodiments of the invention are disclosed below with FIGS. 2 and 3.

...

[0029] The AAA-H verifies the RES the AAA-H received in message 2-6. In this example it is assumed that the verification is successful, and therefore the AAA-H forms, at point 2-7, message 2-8 indicating successful authentication and adds, at point 2-7, to message 2-8 the necessary subscription data, such as whether this subscriber is allowed to obtain a certificate through a mobile network, and the location information of the UE. After that the AAA-H sends message 2-8 to the AU-H. Message 2-8 may be a Diameter message, for example.

[0030] In embodiment one of the invention, the AU-H determines, at point 2-9, the address of the AU-V on the basis of the location information it received in message 2-8. The AU-H preferably comprises a mapping table for pairs formed by the location information and the AU-V address, the mapping table also comprising in embodiment one other relevant information, such as information on the protocol(s) to be used with the AU-V, the public key of the AU-V, a certificate of the AU-V, and/or other security related parameters, for each pair. Another possibility is that the AU-H inquires the address and other relevant information from a network node having the mapping table or corresponding information, the network node being preferably in the home network. The mapping table may comprise only location information with address information, only location information with some relevant information or location information with address information and some relevant information. For example, for location information "operator 1" the mapping table may contain address information, such as certificate.authority@operator1.fi, or a public key, e.g. 123567E97, or both of them. (2004/0166874, pages 2-4, paragraphs 17 and 29-30)

Applicants contend that at least the features of "transmitting to the subscriber's user equipment at least part of information required to obtain a certificate from the certificate provisioning gateway having the address of the certificate provisioning gateway" (which are based on features deemed to be allowable by the Examiner) are not disclosed or suggested by the cited art.

Specifically, RFC 2977 describes requirements which would have to be supported by an Authentication, Authorization, Accounting (AAA) service to aid in providing mobile IP services

(see Abstract of RFC 2977). In discussing with the issue of the use of certificates, RFC 2977 describes that digital certificate can be transported in an AAA message, and states:

3.1. AAA Protocol Roaming Requirements

In this section we will detail additional requirements based on issues discovered through operational experience of existing roaming RADIUS networks. The AAA protocol MUST satisfy these requirements in order for providers to offer a robust service. These requirements have been identified by TR45.6 as part of their involvement with the Mobile IP working group.

...

- Transport a digital certificate in an AAA message, in order to minimize the number of round trips associated with AAA transactions. Note: This requirement applies to AAA applications and not mobile stations. The certificates could be used by foreign and home agents to establish an IPSec security association to secure the mobile node's tunneled data. In this case, the AAA infrastructure could assist by obtaining the revocation status of such a certificate (either by performing online checks or otherwise validating the certificate) so that home and foreign agents could avoid a costly online certificate status check.

(RFC 2977, pages 11-12. Section 3.1)

However, RFC 2977 does not describe that at least part of the information required to obtain certificates through a certificate provisioning gateway authority having an address was determined, at least in part, based on the location of the subscriber's user equipment. Indeed, the Examiner admitted in his rejection of independent claim 2 that "[RFC 2977] **is silent on use of location information AND if they are not the same**, using the address determined on the basis of the location information" (Emphasis in the original, Final Action, page 5), and therefore RFC 2977 must also be silent on use of location information to determine the address of certificate provisioning gateway and/or transmitting information to enable obtaining certificates through the certificate provisioning gateway whose address was determined.

Accordingly, RFC 2977 fails to disclose or suggest at least the features of "transmitting to the subscriber's user equipment at least part of information required to obtain a certificate from the certificate provisioning gateway having the address of the certificate provisioning gateway," as recited in Applicants' independent claim 2.

Tsuda describes a mobile communication system containing mobile node devices according to the Mobile IP protocol and an AAA server device for supporting the mobile node devices according to the AAA protocol (Tsuda, page 1, paragraph 2). Tsuda, however, does not describe transmitting to a subscriber's user equipment information required to obtain a certificate, and Tsuda certainly does not describe transmitting such information to obtain a certificate from a certificate provisioning gateway having an address determined based, at least in part, on the user equipment's location. Accordingly, Tsuda too fails to disclose or suggest at least the features of "transmitting to the subscriber's user equipment at least part of information required to obtain a certificate from the certificate provisioning gateway having the address of the certificate provisioning gateway," as recited in Applicants' independent claim 2.

Lee describes a method and apparatus for supporting nomadic computing of a personal mobility system with transparent virtual networking, information storage, and mobility when the user is traveling from one location to another and/or using different computer platforms or operating modes (Lee, col. 1, lines 14-20). Lee, however, does not describe transmitting to a subscriber's user equipment information required to obtain a certificate. Indeed, Lee makes no mention of any certificate or information relating thereto. Accordingly, Lee too fails to disclose or suggest at least the features of "transmitting to the subscriber's user equipment at least part of information required to obtain a certificate from the certificate provisioning gateway having the address of the certificate provisioning gateway," as recited in Applicants' independent claim 2.

Because none of the references cited by the Examiner discloses or suggests, alone or in combination, at least the features "transmitting to the subscriber's user equipment at least part of information required to obtain a certificate from the certificate provisioning gateway having the address of the certificate provisioning gateway," Applicants' independent claim 2 and the claims depending from it are patentable over the cited art.

Applicant's independent claims 3, 24-26 and 32-35, recite "transmitting to the subscriber's user equipment at least part of information required to obtain a certificate from the certificate provisioning gateway having the determined address," or similar language. For reasons similar to those provided with respect to independent claim 2, Applicants' independent claims 3, 24-26 and 32-35, and the claims depending from them are patentable over the cited art.

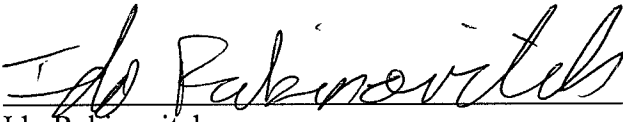
CONCLUDING COMMENTS

It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment. Applicants ask that all claims be allowed.

If there are any questions regarding these amendments and remarks, the Examiner is encouraged to contact the undersigned at the telephone number provided below. The Commissioner is hereby authorized to charge any additional fees that may be due, or credit any overpayment of same, to Deposit Account No. 50-0311, Reference No. 39700-583001US/NC37029US.

Respectfully submitted,

Date: September 1, 2009


Ido Rabinovitch
Reg. No. L0080

Address all written correspondence to
Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.
One Financial Center
Boston, Massachusetts 02111
Customer No. 64046
Telephone: 617-348-1806
Facsimile: 617-542-2241